DEC STD 128-0 Security Classifications for Engineering Intellectual Property — Policy and Regulations

DOCUMENT IDENTIFIER: A-DS-EL00128-00-0000 Rev C, 29-Oct-1991

ABSTRACT: This standard defines Digital policy and requirements for classifying, labeling, storing, and distributing Digital engineering intellectual property that is classified as Digital Restricted Distribution, Digital Confidential, or Digital Internal Use Only.

APPLICABILITY: This standard is mandatory for all Digital employees who handle engineering intellectual property.

STATUS: APPROVED 29-Oct-1991; use VTX SMC for current status.

This document is confidential and proprietary, and is the property of Digital Equipment Corporation. It is an unpublished work protected under applicable copyright laws.

© Digital Equipment Corporation. 1990, 1991. All rights reserved.

DEC STD 128-0 Security Classifications for Engineering Intellectual Property — Policy and Regulations

DOCUMENT IDENTIFIER: A-DS-EL00128-00-0000 Rev C, 29-Oct-1991

REVISION HISTORY:	Rev A,	04-Sep-1980	
	Rev B,	31-Jan-1990	ECO Number CTS01
	Rev C,	29-Oct-1991	ECO Number NRO02

Document Management Category:	Cross Documentation Vocabulary and Practices (TDV)
Responsible Department:	Office of Engineering Security
Responsible Person:	David Hamilton
SMC Writer:	C.J. Keating

APPROVAL: This document has been reviewed and recommended for approval by the General Review group for its category.

David Hamilton - Standard Owner

Eric Williams - Standards Process Manager

Direct requests for further information to:

Bill Pozerycki
Use $ VTX ELF for the latest location information.

Use VTX SMC to order copies of this document from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

CONTENTS

1 INTRODUCTION 1
1.1 PURPOSE 1
1.2 SCOPE 1
1.3 RESPONSIBILITIES 2
1.3.1 When To Classify 2
1.3.2 Responsible Engineers 2
1.3.3 Originators 2
1.3.4 Design Libraries and Document Control 3
1.3.5 Micrographic Services 3
1.3.6 Microfilm Reference Libraries 3
1.3.7 Engineering Services 3
1.3.8 Office of Engineering Security 3
1.4 THIRD-PARTY CONFIDENTIAL INFORMATION 3

2 CLASSIFICATIONS 4
2.1 DIGITAL RESTRICTED DISTRIBUTION 4
2.2 DIGITAL CONFIDENTIAL 5
2.3 DIGITAL INTERNAL USE ONLY 5
2.4 INFORMATION CONTAINING NO RESTRICTIONS 6

3 GOVERNMENT REQUIREMENTS 7
3.1 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR) 7

4 MARKING REQUIREMENTS 8
4.1 HARD COPY 8
4.2 COMPUTER READABLE MEDIA 8
4.3 MICROFILM 8
4.4 NETWORK DATA 8
4.5 ENGINEERING DRAWINGS 9
4.6 ENGINEERING NOTEBOOKS 9

5 ACCOUNTABILITY FOR DIGITAL RESTRICTED DISTRIBUTION 10
5.1 ORIGINATOR 10
5.2 INCOMING LOG 12
5.3 RETURN RECEIPT 14
5.4 COVER SHEET 15
5.5 COPYING AND REPRODUCTION 15
5.6 OFFSITE STORAGE OF TAPES, DISKS 15

6 DISTRIBUTION 17
6.1 DIGITAL RESTRICTED DISTRIBUTION 17
6.2 DIGITAL CONFIDENTIAL 18
6.3 DIGITAL INTERNAL USE ONLY 18

7 STORAGE AND PROTECTION 19

8 RECLASSIFICATION 20

9 PROPRIETARY WASTE AND DISPOSAL 20
10 COMPROMISE OR LOSS OF PROPRIETARY INFORMATION 20
11 FIELD MAINTENANCE PRINT SET RESTRICTIONS 20

Appendix A REFERENCED DOCUMENTS 21
A.1 EL-Class Digital Documents 21
A.2 Other Digital Documents 21
A.3 Ordering Information 21

FIGURES

1 Digital Restricted Distribution Originator's Log Example 11
2 Digital Restricted Distribution Incoming Log Example 13
3 Digital Restricted Distribution Return Receipt Example 14
4 Digital Restricted Distribution Cover Page Example 16

1 INTRODUCTION

This standard provides an engineering interpretation of Corporate Security Policy 10.0, *Information Security Policy*. It is strongly recommended that you also read Corporate Security Standard 10.1, *Information Security*.

Any description of a product, research, or a project or process to produce the same, is Digital's engineering intellectual property. Any Digital product or research incorporates the ideas of Digital employees (or nonemployees working on behalf of Digital), and therefore is deemed engineering intellectual property. In many cases, other third-party information received by Digital is considered engineering intellectual property as defined in this standard.

Most of Digital's engineering intellectual property is controlled and distributed by any of the following organizations.

- Corporate Micrographics
- Standards and Methods Control
- Engineering Services Design Libraries
- Groups that supply or support software

All engineering intellectual property must be identified with the standard proprietary disclaimer and copyright notice. If it is to be made available to outside sources, the content should be reviewed by the originator to prevent disclosure of sensitive information.

Security classifications are intended to protect sensitive engineering intellectual property. The proper classifications of all products and research-related materials must be identified to ensure adequate protection of Digital's investments. The classification and labeling of Digital property as **Digital Restricted Distribution**, **Digital Confidential**, or **Digital Internal Use Only** indicates that special handling must occur. Not all engineering intellectual property must be classified (see subhead 2.4).

1.1 PURPOSE

This standard defines the classification policy and requirements for labeling, storing, and distributing engineering intellectual property.

1.2 SCOPE

Digital classifies engineering information in one of four ways.

1. **Digital Restricted Distribution**
2. **Digital Confidential**
3. **Digital Internal Use Only**
4. Information containing no restrictions, but with a standard disclaimer and copyright notice.

The scope of this standard is generally limited to engineering information that is classified as **Digital Restricted Distribution, Digital Confidential**, or **Digital Internal Use Only**. This information includes, but is not limited to, anything that requires an engineering documentation number per *DEC STD 012-1 Documentation Identification Conventions, Including Mnemonic Codes*. Head 3 of this standard includes information on government requirements for handling information.

This standard establishes the criteria for classifying engineering intellectual property as **Digital Restricted Distribution**, **Digital Confidential**, or **Digital Internal Use Only**. It defines responsibility for compliance and describes the handling, labeling, distribution, and treatment of the following types of property.

- Software used to generate product information
- Machine-readable product information
- Hard copy product information

The requirements of this standard are effective on the standard's approval date, applying to all newly created or changed engineering intellectual property.

1.3 RESPONSIBILITIES

Every employee who handles Digital engineering intellectual property is responsible for abiding by the requirements of this standard. Specific responsibilities are designated in the following paragraphs.

1.3.1 When To Classify

The time to classify engineering intellectual property is at the earliest time (in the conceptual stage) that property is recognized as valuable to the company.

1.3.2 Responsible Engineers

Responsible engineers (or responsible persons) must determine the correct classifications for their product design information and other engineering intellectual property.

1.3.3 Originators

Originators must determine the appropriate classification category for information originated by them, as assigned to them, or under their custody from any third party.

Originators must provide a continuous degree of protection, from creation to destruction, consistent with the requirements of this standard and Corporate Security Standard 10.1.

Originators must also determine the appropriate distribution of proprietary information consistent with "need-to-know" criteria.

The originator of an engineering document that is to be classified **Digital Restricted Distribution** or **Digital Confidential** is responsible for identifying the responsible engineer, who will in turn authorize the reproduction and release of the document and inform the Design Library holding the original.

1.3.4 Design Libraries and Document Control

Design libraries and document control groups are responsible for storing all engineering intellectual property at their geographic location in accordance with the storage requirements of this standard.

1.3.5 Micrographic Services

Corporate Micrographic Services is responsible for the microfilming of all documentation in the Engineering Documentation System, and maintaining a master file of **Digital Restricted Distribution** and **Digital Confidential** silver negatives in accordance with the requirements of this standard.

1.3.6 Microfilm Reference Libraries

Microfilm reference libraries are responsible for storing a blank image on an aperture card whenever a document is classified **Digital Restricted Distribution**.

1.3.7 Engineering Services

It is the responsibility of Engineering Services sites or other organizations that prepare documentation for the Engineering Documentation System to ensure that a document classified **Digital Restricted Distribution, Digital Confidential,** or **Digital Internal Use Only** is labeled and handled in accordance with the requirements of this standard.

1.3.8 Office of Engineering Security

Office of Engineering Security is responsible for the content of this standard. Any requests to change this standard must be submitted to the Office of Engineering Security.

1.4 THIRD-PARTY CONFIDENTIAL INFORMATION

Customer and supplier confidential information normally is provided to Digital for a limited purpose. This information is referred to as "Third-Party Confidential Information". The user of this information should be familiar with the terms and conditions of Digital's contract with the customer or supplier. If the user is not certain of the right to use or disclose third-party information, then the information should be treated as **Digital Confidential**.

Third-Party Confidential Information shall be marked on the top and bottom of the first page and on the bottom of all other pages, with the special Third-Party Confidential Information label. The label is available from the local security organizations.

2 CLASSIFICATIONS

The classification of information as **Digital Restricted Distribution**, **Digital Confidential**, or **Digital Internal Use Only**, can often be related to timing as well as to the content of the information. For instance, information about new products being developed and tested should not be published until after a public announcement is made.

NOTE

Other types of highly sensitive information such as customer lists, trade secrets, and proprietary manufacturing processes, should not be published.

Information derived from a classified document must be classified the same as the original document, unless the originator reviews the extract and approves the reclassification of the finished product. This pertains to all charts, memos, project drawings, code names, and technical and financial data associated with the document.

Digital classified proprietary information shall be distributed only to employees who have a need to know. Recipients of such material have the responsibility to ensure that further dissemination is based on the need-to-know principle. It is incumbent on all employees to ensure that distribution lists for classified proprietary information contain only the names of individuals who have been determined to have a need to know for the material being disseminated.

All engineering intellectual property bearing one of the three security classifications defined in this standard must contain the standard statement and copyright notice shown below.

> This document is confidential and proprietary, and is the property of Digital Equipment Corporation. It is an unpublished work protected under applicable copyright laws.
>
> © Digital Equipment Corporation. 199n. All rights reserved.

If the device or the editing tool cannot represent the copyright symbol (©), use the following line instead.

> Copyright (c) Digital Equipment Corporation. 199n. All rights reserved.

DEC STD 197-0 Legal Requirements and Guidelines for Digital Publications and Software provides general guidelines and information on copyright and disclaimer statements.

2.1 DIGITAL RESTRICTED DISTRIBUTION

This is the highest Digital classification category. Information labeled **Digital Restricted Distribution** indicates that its unauthorized or inadvertent disclosure could cause serious damage to the operation of the corporation; its use and distribution must be severely restricted. The assignment of this classification is a subjective judgment on the part of the originator. This category includes the most sensitive plans, ideas, research and development activities and similar information that only a few people within the corporation have an absolute need to know.

EXAMPLE

Unannounced new product specifications, key technical concepts and processes, code names, manufacturing processes and information required by law to be preserved or shielded under the highest classification system. Sensitive proprietary information that vendors or customers give us may be put in this category, if stipulated by contract and/or negotiated agreement.

2.2 DIGITAL CONFIDENTIAL

The mid-level classification for proprietary information, **Digital Confidential,** indicates that unauthorized or inadvertent disclosure could have a substantially detrimental effect on the operation of the Company. This is information that is sensitive to Digital and normally associated with a particular process, project, or function, the very nature of which requires limited need-to-know distribution.

EXAMPLE

Subsystem designs, plans pertaining to most products under development, and similar items received from outside sources may also fall within this category (organizational legal support should be consulted in questions of doubt).

2.3 DIGITAL INTERNAL USE ONLY

This proprietary information classification indicates that unauthorized or inadvertent disclosure could cause business damage to the Corporation. It can be distributed to Digital employees but must not be given to anyone who is not an employee of Digital, including but not limited to customers, competitors, vendors, or other persons or organizations without originator authorization, and the execution of the appropriate nondisclosure agreement.

EXAMPLE

Select Digital engineering policies, standards, and procedures, daily operational memos, and select drawings are examples of documents in this category.

2.4 INFORMATION CONTAINING NO RESTRICTIONS

Some engineering intellectual property, especially material prepared for external distribution, may not bear one of the three security classifications previously mentioned in this section but must contain one of the following standard statements and copyright notices.

> The drawing and specifications, herein, are the property of Digital Equipment Corporation and shall not be reproduced, copied, or used in whole or in part as the basis for the manufacture or sale of items without written permission.
>
> © Digital Equipment Corporation. 199n. All rights reserved.

> This document is the property of Digital Equipment Corporation and shall not be reproduced, copied, or used in whole or in part as the basis for the manufacture or sale of items without written permission.
>
> © Digital Equipment Corporation. 199n. All right reserved.

If the device or the editing tool cannot represent the copyright symbol (©), use the following line instead.

> Copyright (c) Digital Equipment Corporation. 199n. All rights reserved.

3 GOVERNMENT REQUIREMENTS

National governments and alliance organizations of governments (such as NATO, European Community) may impose additional requirements on the handling of sensitive information. This includes:

- How sensitive information belonging to the government is handled while being used within Digital, and
- How we must label Digital information given to governments to ensure that it is properly handled within that government

3.1 INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

The International Traffic in Arms Regulations were issued by the United States Department of State for products built to military specifications or for military applications. These regulations apply to all (U.S. and non-U.S.) product managers and engineers regardless of the intended destination of the product.

- **Responsible Engineers (or Responsible Persons)** must obtain the correct export classifications for their product design information and other engineering intellectual property from Corporate Export.
- **Originators** of information must provide details of technical capabilities to Corporate Export for export classification. Originators must further ensure that any product classified by Corporate Export as "ITAR controlled" is marked as such on all documents and transmissions. In addition, originators must ensure that all technical information is distributed on a limited basis, as determined by Area Export, in compliance with ITAR.
- **Design Libraries and Document Control** are responsible for ensuring that all documents marked as ITAR controlled are distributed only after screening the requester and the intended end use against a specific set of criteria. Contact your Area Export group for screening criteria.
- **Microfilm Reference Libraries** are responsible for storing an ITAR-unique message/image on an aperture card and for screening requesters with the support and approval of Area Export prior to releasing.
- **Engineering Services** is responsible for marking all generated documents with the words "ITAR controlled".

Any questions related to the ITAR requirements should be directed to either Area Export or Corporate Export.

4 MARKING REQUIREMENTS

The originator of Digital engineering intellectual property will ensure that the appropriate classification marking is shown on the document as described in the following subheads.

Documents designated **Digital Restricted Distribution** will also require a log number marking on the cover sheet. Details of this marking are discussed in subhead 5.4, and shown in Figure 4.

4.1 HARD COPY

Computer printouts, volume runs, vendor-printed material, and so forth, shall have the classification marking displayed on the top and bottom of the first page (or title page), and front and back covers if a bound document. The classification marking should be at the bottom of each page of a volume run or other unbound document. The person generating the hard copy is responsible for applying the classification label even if it is handwritten. All labeling of hard copies must be readable when hand held.

4.2 COMPUTER READABLE MEDIA

Magnetic tapes, floppy disks, diskpacks, or other storage devices that contain sensitive proprietary information will have the appropriate classification marking affixed by use of a stick-on label on the outer shell or container. The classification also should be stored electronically on the media.

4.3 MICROFILM

Microfilm aperture cards of **Digital Restricted Distribution** drawings are not to be distributed to microfilm reference libraries. Instead, a substitute card without image is distributed to the film library indicating that the document is classified **Digital Restricted Distribution** and may be obtained from Corporate Micrographics only on a need-to-know basis when authorized by the responsible engineer.

4.4 NETWORK DATA

All network data shall display its Digital security classification label, both in the screen display and the produced data (calculations, reports, and so forth). For specific instructions, see Corporate Security Standard 11.1, *Computer Security*.

4.5 ENGINEERING DRAWINGS

All engineering drawings are engineering intellectual property and must be classified in one of the classifications prescribed by this standard. Such classification markings will be prominently displayed in the upper-left corner of the drawing. All engineering drawings will also display the standard statement and copyright notice shown in subhead 2.4. This marking will also appear in the upper-left corner of the drawing. See *DEC STD 013-0 Standard Engineering Drawing Formats and Forms* for further information.

4.6 ENGINEERING NOTEBOOKS

The Engineering Notebook is the property of Digital Equipment Corporation. It is a specially formatted, hard-bound notebook used to record the conception and development of potentially patentable ideas and other engineering activities, notes, calculations, sketches, data, and so forth. It often contains highly sensitive and valuable information. For this reason, all information contained within the notebook must be classified and handled in accordance with this standard. The appropriate classification must be prominently marked on the top and bottom of each page containing information classified as such. For more information, see *DEC STD 141-0 Engineering Notebook Policy and Requirements*.

5 ACCOUNTABILITY FOR DIGITAL RESTRICTED DISTRIBUTION

All **Digital Restricted Distribution** material requires special handling within the Corporation, far above that normally provided for other proprietary information. Accordingly, this category of classified material requires a special logging system, which shall be maintained by each originator and recipient in order to provide a continuous audit trail.

The aforementioned procedure does not apply to other classification categories. There are no logging or other special accountability requirements for the other classification categories.

5.1 ORIGINATOR

Regardless of how the material is transmitted, the originator of such a document must maintain a log of each copy. A sample of the Originator's Log is shown in Figure 1, showing entries for the following items.

- The Document Control Number is the year/cost center/document number; for example, 1991-68R-001.
- The Title is the subject of the document.
- The Date is the document date or origination date.
- The Copy No. is the number assigned to each copy of the document produced; for example, Copy 1 of 20.
- The Addressee is the name of the person to whom the copy was sent.
- The Certified or Reg. Mail No. is the postal authority number assigned for external mail use. If internal mail is used, this column is blank.
- The Date Return Receipt Rec'd shows the actual date that the document was received by the addressee.
- When the document is destroyed, the destruction date and person who actually accomplished the destruction will be shown in the addressee column above other entries, and a single line will be drawn through the log entry.

Figure 1: Digital Restricted Distribution Originator's Log Example

DIGITAL RESTRICTED DISTRIBUTION

Originator's Log

Document Control Number	Title	Date	Copy No.	Addressee	Certified or Reg. Mail No.	Date Return Receipt Rec'd

5.2 INCOMING LOG

Each recipient of **Digital Restricted Distribution** material must maintain an Incoming Log of each document received. A sample of this log is shown in Figure 2, showing entries for the following items.

- The Document Control Number is the number assigned by the originator. If the cost center receiving the document determines that additional copies are absolutely required, the cost center must receive written permission from the originator before copies can be made.
- The Title is the subject of the document.
- The Date is the date on the document.
- The Copy No. is the number assigned to each copy of the document produced; for example, copy 1 of 20.
- The Originator is the person or cost center originating the document.
- The Mail No. is the external mail number used by postal authorities. It does not apply for internally mailed material.
- The Date Rec'd is the date the document arrived at the cost center.
- The Rec'd From will be filled in when the name is different from the originator.
- Disposition is the current location of the document (a pencil entry until destruction occurs). Upon destruction, the date and person destroying the document will be entered here.

The recipient of each copy is responsible for ensuring that the copy is secured out of sight. Each copy is for the eyes of the recipient only, and all copy requests should be forwarded to the originator. It is up to the originator to determine if the requester has a need to know.

Figure 2: Digital Restricted Distribution Incoming Log Example

DIGITAL RESTRICTED DISTRIBUTION

Incoming Log

Document Control Number	Title	Date	Copy No.	Originator	Mail No.	Date Rec'd	Rec'd From	Dis-position

5.3 RETURN RECEIPT

All **Digital Restricted Distribution** material will have a return receipt (Figure 3) attached to the material. The addressee will sign the receipt indicating the document arrived as sent, and return the receipt to the originator. Return receipts will be audited by the originator to ensure that everyone received their copy.

Figure 3: Digital Restricted Distribution Return Receipt Example

DIGITAL RESTRICTED DISTRIBUTION

RETURN RECEIPT

* * * PLEASE RETURN * * *

Document Control Number: 1991-68R-001

TO TRACK THE MAILING AND DISTRIBUTION OF THE DOCUMENT, PLEASE RETURN THIS RECEIPT TO THE ORIGINATOR AS SOON AS YOU RECEIVE THE DOCUMENT.

YOUR NAME: _____

YOUR BADGE NUMBER: _____

SIGNATURE: _____

DATE: _____

DOCUMENT NUMBER: _____

COPY NUMBER: _____

5.4 COVER SHEET

Each copy of a **Digital Restricted Distribution** document must have a cover sheet. A sample cover sheet is shown in Figure 4, showing entries for the following information.

- The **Digital Restricted Distribution** classification (top and bottom)
- Title
- Date
- Document control number is the year / cost center / document number; for example, 1991-68R-001
- Copy number of this copy
- Total number of copies of this restricted distribution list
- Name of the recipient of this copy
- Name of the originator

The words "ITAR controlled" shall be marked on the cover sheet if the document has been classified as ITAR controlled.

The copy number shall be marked in the bottom-right corner of the title page or first page of a document, or on the separate stick-on label for hardware or tapes.

5.5 COPYING AND REPRODUCTION

The recipient must not copy or reproduce **Digital Restricted Distribution** material. All copies must be requested from the originator to enable proper tracking procedures.

5.6 OFFSITE STORAGE OF TAPES, DISKS

The **Digital Restricted Distribution** classification marking and its control number will be visible on the outside of the container or package when stored offsite. Receipts for the material must also be obtained.

Figure 4: Digital Restricted Distribution Cover Page Example

Digital Restricted Distribution

Title: Communications Systems Architecture

Document Control Number: 1991-68R-001

Originator: X.G. Keys

Date: 03-Oct-1991

Addressee: _____

Copy _____ of 20

Digital Restricted Distribution

6 DISTRIBUTION

This section discusses the means of distribution for Digital engineering intellectual property classified as **Digital Restricted Distribution**, **Digital Confidential**, and **Digital Internal Use Only**.

6.1 DIGITAL RESTRICTED DISTRIBUTION

Digital Restricted Distribution material should not be transmitted by electronic means but in hard copy format. This provision is subject to future review when full encryption capability exists within the Corporation. If an originator decides not to follow this recommendation (because of a business decision to take the risk to achieve greater speed), all known precautions should be taken as recommended in Corporate Security Standard 11.1.

Information classified **Digital Restricted Distribution** must be double-wrapped when sent through the mail. The following applies.

- **External Mail**: The material will be placed in an inner envelope marked with the name and address of the addressee, marked *TO BE OPENED BY ADDRESSEE ONLY*, and displaying the appropriate classification marking. The outer envelope will be opaque and will show only the name and address of the addressee. Additionally, **Digital Restricted Distribution** material will be mailed by U.S. certified or registered mail, with a return receipt required. An equivalent method may be used in other countries to ensure that the document is tracked to its destination, and the originator is notified.
- **Internal Digital Mail**: The material will be placed in an inner envelope marked with the name and address of the addressee, marked *TO BE OPENED BY ADDRESSEE ONLY*, and displaying the appropriate classification marking. The outer envelope will be opaque and will show only the name and address of the addressee.

Information classified **Digital Restricted Distribution** may be sent in containers other than the standard envelope (boxes or shipping tubes). If a box or tube is used, no inner envelope is required unless several items in that outer envelope are meant for distribution to more than one addressee.

When it is absolutely necessary to use mailing and/or distribution lists for recurring dissemination of proprietary information, originators must ensure that such lists only contain the names of individuals with a need to know. All such lists should be updated monthly for **Digital Restricted Distribution** information.

6.2 DIGITAL CONFIDENTIAL

Digital Confidential material can be transmitted by electronic means. However, all known precautions should be taken as recommended in Corporate Security Standard 11.1.

Information classified **Digital Confidential** must be double-wrapped when sent through the mail. The following applies.

- **External Mail**: The material will be placed in an inner envelope which will be marked with the name and address of the addressee, marked *TO BE OPENED BY ADDRESSEE ONLY*, and display the appropriate classification marking. The outer envelope will be opaque and will show only the name and address of the addressee.
- **Internal Digital Mail**: The material will be placed in an inner envelope which will be marked with the name and address of the addressee, marked *TO BE OPENED BY ADDRESSEE ONLY*, and display the appropriate classification marking. The outer envelope will be opaque and will show only the name and address of the addressee.

Information classified **Digital Confidential** may be sent in containers other than the standard envelope (boxes or shipping tubes). If a box or tube is used, no inner envelope is required unless several items in that outer envelope are meant for distribution to more than one addressee.

When it is absolutely necessary to use mailing and/or distribution lists for recurring dissemination of proprietary information, originators must ensure that such lists contain only the names of individuals with a need to know. All such lists should be updated quarterly for **Digital Confidential** information.

6.3 DIGITAL INTERNAL USE ONLY

Digital Internal Use Only material may be sent through regular mail channels without special markings on the mailing containers or envelopes.

7 STORAGE AND PROTECTION

The quantity and sensitivity of proprietary information often determines the methods and requirements for protection of the material. A research and development facility housing thousands of documents, all of which may be very sensitive, will require more secure storage than a small sales office with only one document. For a facility with a large number of sensitive documents, enhanced site-wide (controlled project areas) or project security measures should be considered. The establishment of restricted areas may be a valid alternative to the provision of individual secure storage containers.

Digital Restricted Distribution: Must be placed in a secure container or safe that is locked when unattended. Must not be left exposed on desks, file tops, tables, and so forth. If stored in a file cabinet or office desk, the cabinet or desk must be equipped with a bar and lock or similar device that precludes a drawer being opened more than 3.2 mm (0.13 in) when closed or locked.

Digital Confidential: Must be filed or stored in a locked desk or file cabinet. Must not be left exposed on desks, file tops, tables, or otherwise exposed, unless in a secure or controlled area dedicated to a major project.

Digital Internal Use Only: No special storage requirements when maintained on Digital property. Should be stored in a locked container or be in the possession of a Digital employee at all times when off Digital property.

Digital Restricted Distribution and **Digital Confidential** material or media stored offsite will be segregated from other tapes, disks, or material and secured in a locked cabinet or safe. If the volume prohibits such protection, then a secure room will be used with floor-to-ceiling walls, an alarm system to detect unauthorized intrusion, and enforced access controls. Offsite storage locations will be inspected and approved by the appropriate line organization Digital security representative. Vendors must agree to the foregoing before offsite storage begins. They must also sign a nondisclosure agreement.

The above represents the minimum standards required for the protection of a limited quantity of proprietary information. Larger quantities may require additional protection, such as vaults or tamper-resistant combination locks on safes. Your Security representative can help you evaluate your requirements.

8 RECLASSIFICATION

During its lifetime, the value of engineering intellectual property may change. Therefore, reclassification may be necessary, but any released product requires an ECO to reclassify.

9 PROPRIETARY WASTE AND DISPOSAL

All classified waste will be destroyed in such a manner that documents are rendered unreadable, and hardware, microfiche, microfilm and related materials are rendered unrecognizable and not usable. Document shredders, disintegrators, burning, and so forth, are approved methods of destruction.

There must be a record made of the destruction of **Digital Restricted Distribution** material. An entry is required in the Incoming Log to indicate the date of destruction and the person destroying the material.

If an outside vendor is selected to destroy Digital's proprietary information, the following shall be adhered to.

- The vendor will sign a nondisclosure agreement.
- The vendor will agree to announced and unannounced inspections of the storage and destruction sites.
- The vendor will agree to physical security requirements as defined by Digital. If the vendor does not comply with these guidelines, then the contract shall be voided.
- An initial security review will be conducted by the Digital line organization security function prior to finalizing the contract, to ensure that the vendor can comply with appropriate destruction requirements. A written record of this review will be maintained by the security function.

10 COMPROMISE OR LOSS OF PROPRIETARY INFORMATION

Digital employees who become aware of the compromise or loss of **Digital Restricted Distribution** or **Digital Confidential** information will report this fact to their manager. Managers will report such instances to the Office of Engineering Security and the originator of the document.

11 FIELD MAINTENANCE PRINT SET RESTRICTIONS

No document (printed hard copy or computer media) classified as **Digital Restricted Distribution, Digital Confidential,** or **Digital Internal Use Only** shall be published as part of a field maintenance print set or microfilm file. For further information on the security of field maintenance print sets, see *DEC STD 117-0 Print Sets*.

APPENDIX A REFERENCED DOCUMENTS

A.1 EL-Class Digital Documents

EL-Class Number	Document Title
EL-00012-01	*DEC STD 012-1 Documentation Identification Conventions Including Mnemonic Codes*
EL-00013-00	*DEC STD 013-0 Standard Engineering Drawing Formats and Forms*
EL-00117-00	*DEC STD 117-0 Print Sets*
EL-00141-00	*DEC STD 141-0 Engineering Notebook Policy and Requirements*
EL-00197-00	*DEC STD 197-0 Legal Requirements and Guidelines for Digital Publications and Software*

Use VTX SMC to order copies of EL-class documents from Standards and Methods Control. Send distribution questions to JOKUR::SMC or call DTN: 234-4423.

A.2 Other Digital Documents

Document Number	Document Title
	Corporate Security Policy 10.0, Information Security Policy
	Corporate Security Standard 10.1, Information Security
	Corporate Security Standard 11.1, Computer Security

A.3 Ordering Information

Following are the sources for documents not available from Standards and Methods Control.

- Copies of Corporate Security documents may be obtained by accessing VTX SECURITY_POLICY.

```
+---------------------------------------------------------------------+
|                          READER COMMENTS                            |
|                                                                     |
| Your  comments  and suggestions  will help  Standards and Methods   |
| Control improve their services and documents.                       |
+---------------------------------------------------------------------+
```

Did you request this document? _____ If so, did it arrive within a satisfactory period of time? _____ Please comment.

What are your impressions of this document? Consider format, organization, completeness, readability, and illustrations.

————————————**FOLD ON THIS LINE**———————————————————————— -

Did you find technical or clerical errors in this document? If so, please specify the page number(s) and the error(s).

Are the instructions for the update package clear? _____
Was an index available? _____ If not, is one needed? _____
Do you have other suggestions for improving this document?

The following information is optional:

Name _____ Mailstop _____

Department _____ Node _____

Send your comments to JOKUR::PROJECTS, or fold, staple, and send this page through interoffice mail to:

```
+------------------------------+
|       READERS' COMMENTS      |
| STANDARDS AND METHODS CONTROL |
|           NRO4/D4            |
+------------------------------+
```